FIG. 1

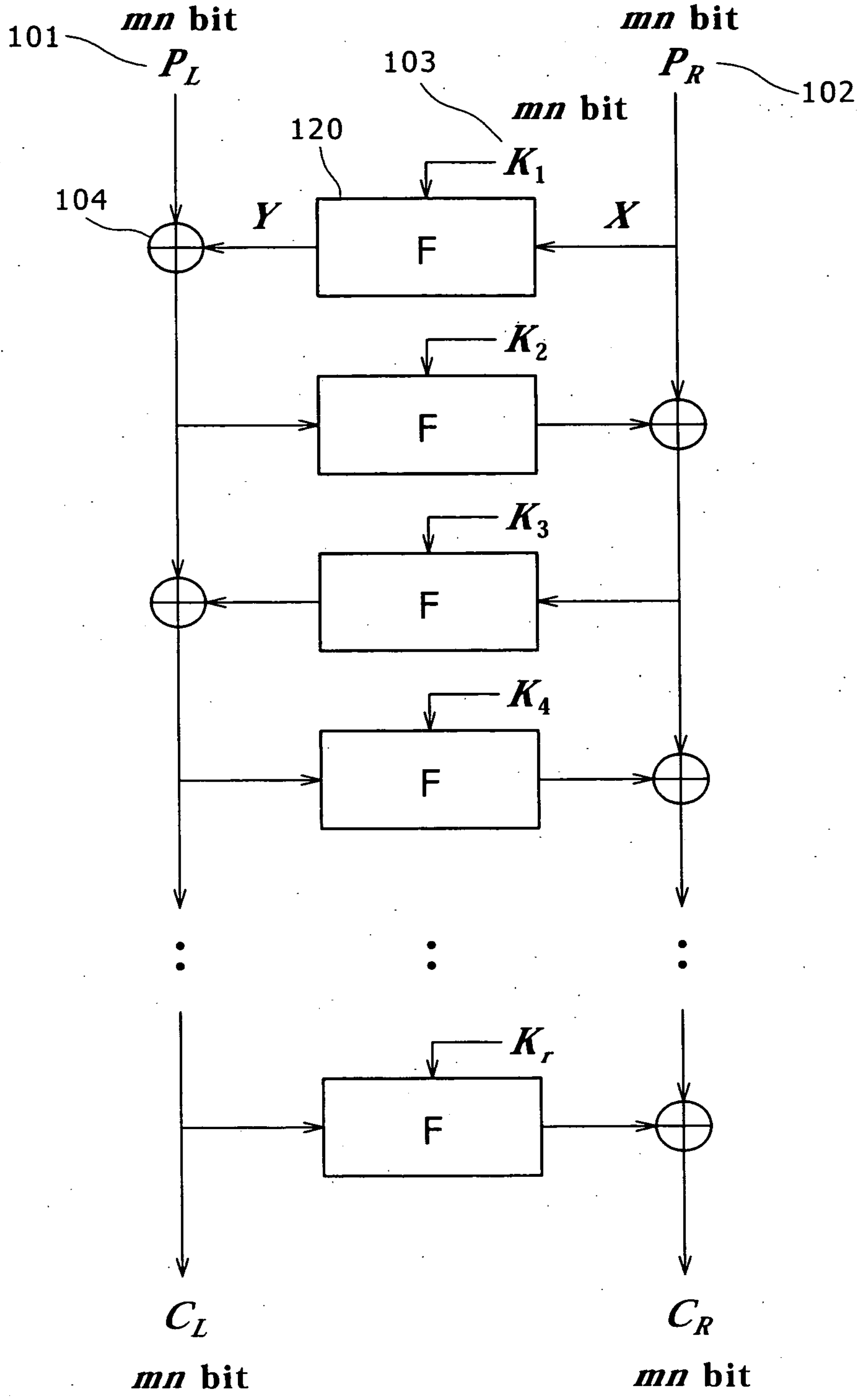

101
mn bit
P_L
103
mn bit
K_1
mn bit
P_R
102
120
104
Y
F
X
K_2
F
K_3
F
K_4
F
K_r
F
C_L
mn bit
C_R
mn bit

FIG. 2A

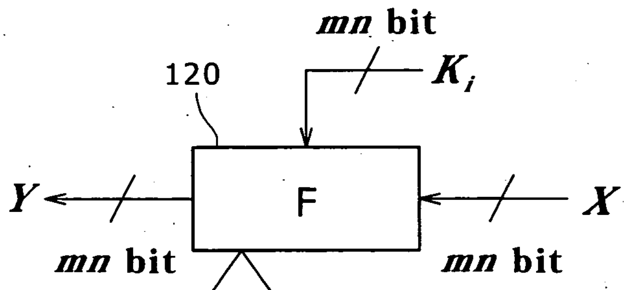

mn bit
120
K_i
Y
F
X
mn bit
mn bit

FIG. 2B

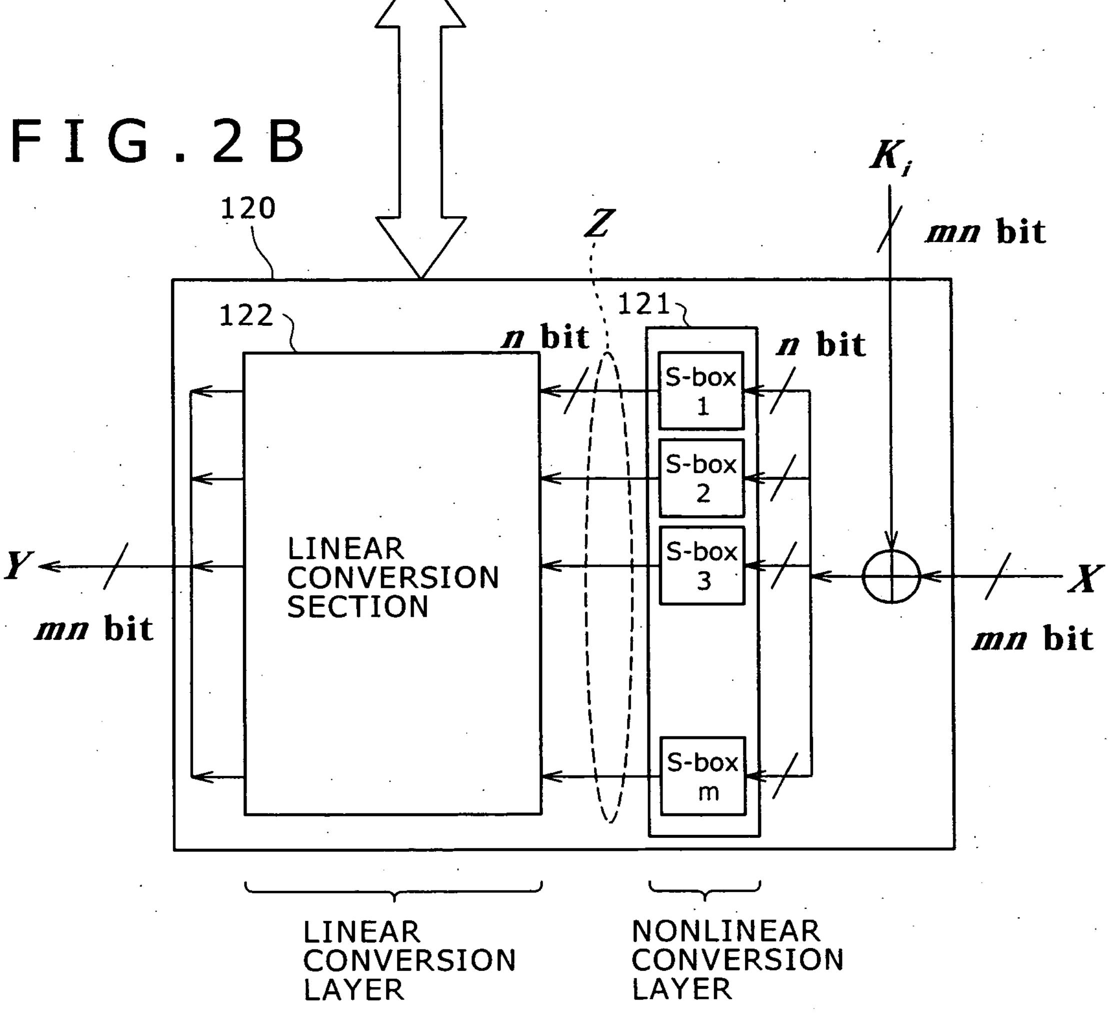
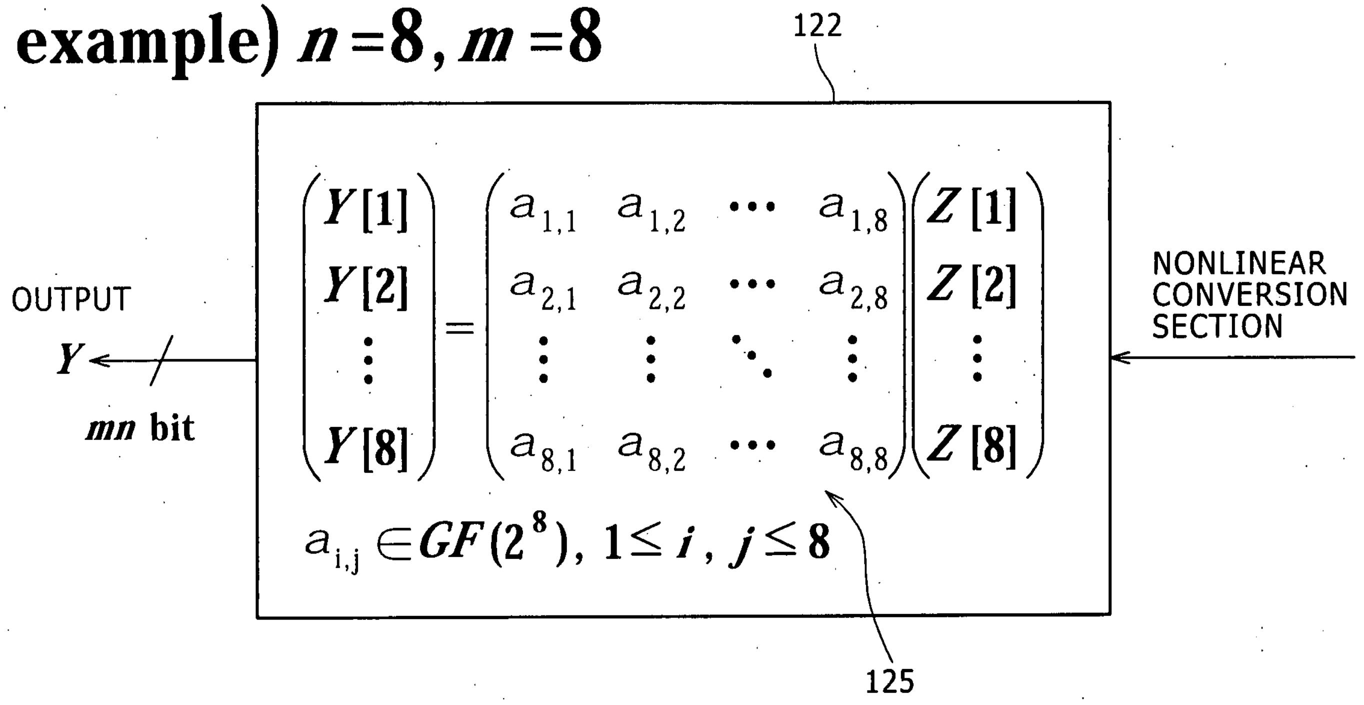

K_i
mn bit
120
Z
121
122
n bit
n bit
S-box 1
S-box 2
S-box 3
S-box m
LINEAR CONVERSION SECTION
Y
mn bit
X
mn bit
LINEAR CONVERSION LAYER
NONLINEAR CONVERSION LAYER

FIG.3

example) $n=8, m=8$



$$\begin{pmatrix} Y[1] \\ Y[2] \\ \vdots \\ Y[8] \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,8} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ a_{8,1} & a_{8,2} & \cdots & a_{8,8} \end{pmatrix} \begin{pmatrix} Z[1] \\ Z[2] \\ \vdots \\ Z[8] \end{pmatrix}$$

$$a_{i,j} \in GF(2^8),\ 1 \leq i,\ j \leq 8$$

FIG. 4

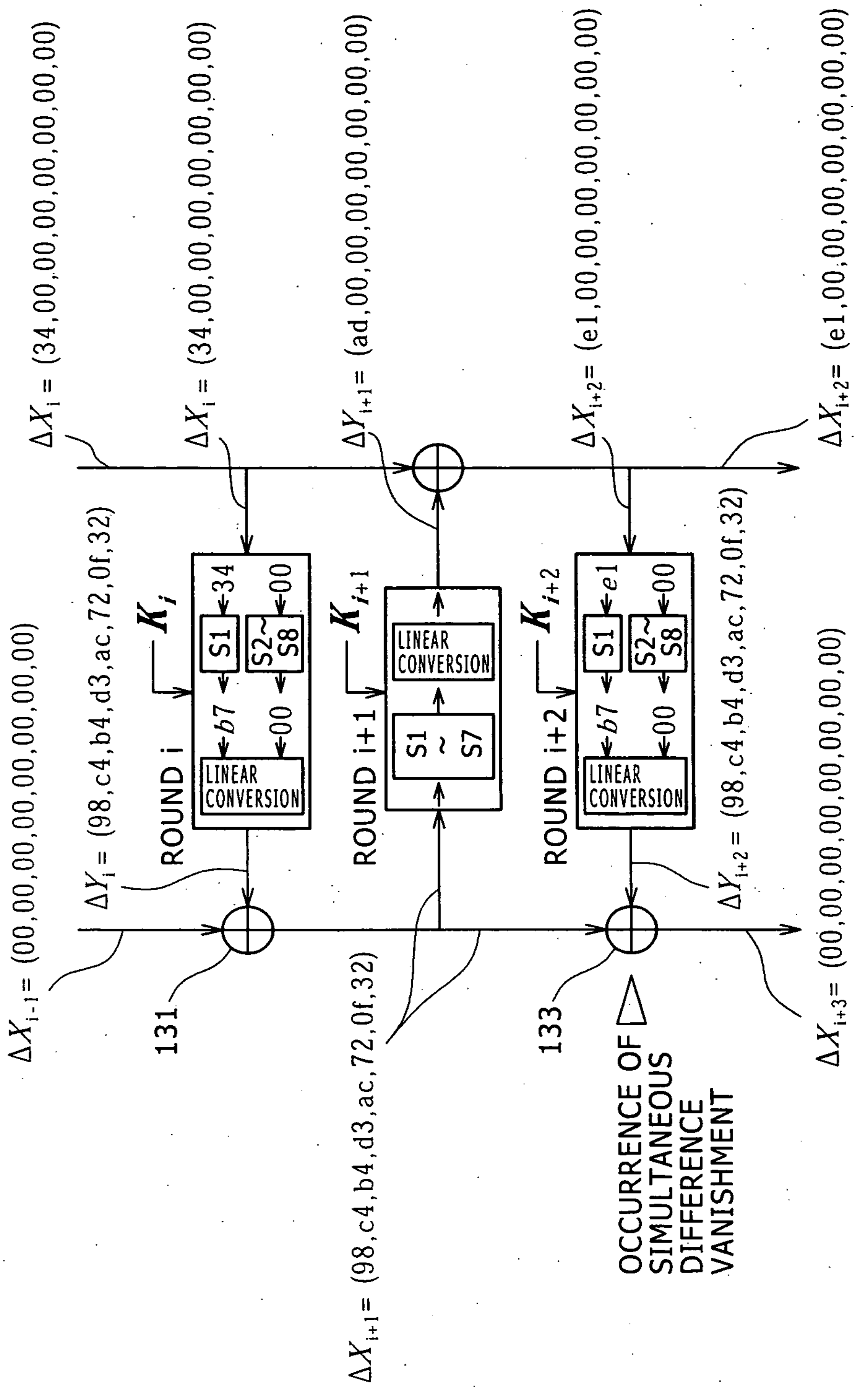
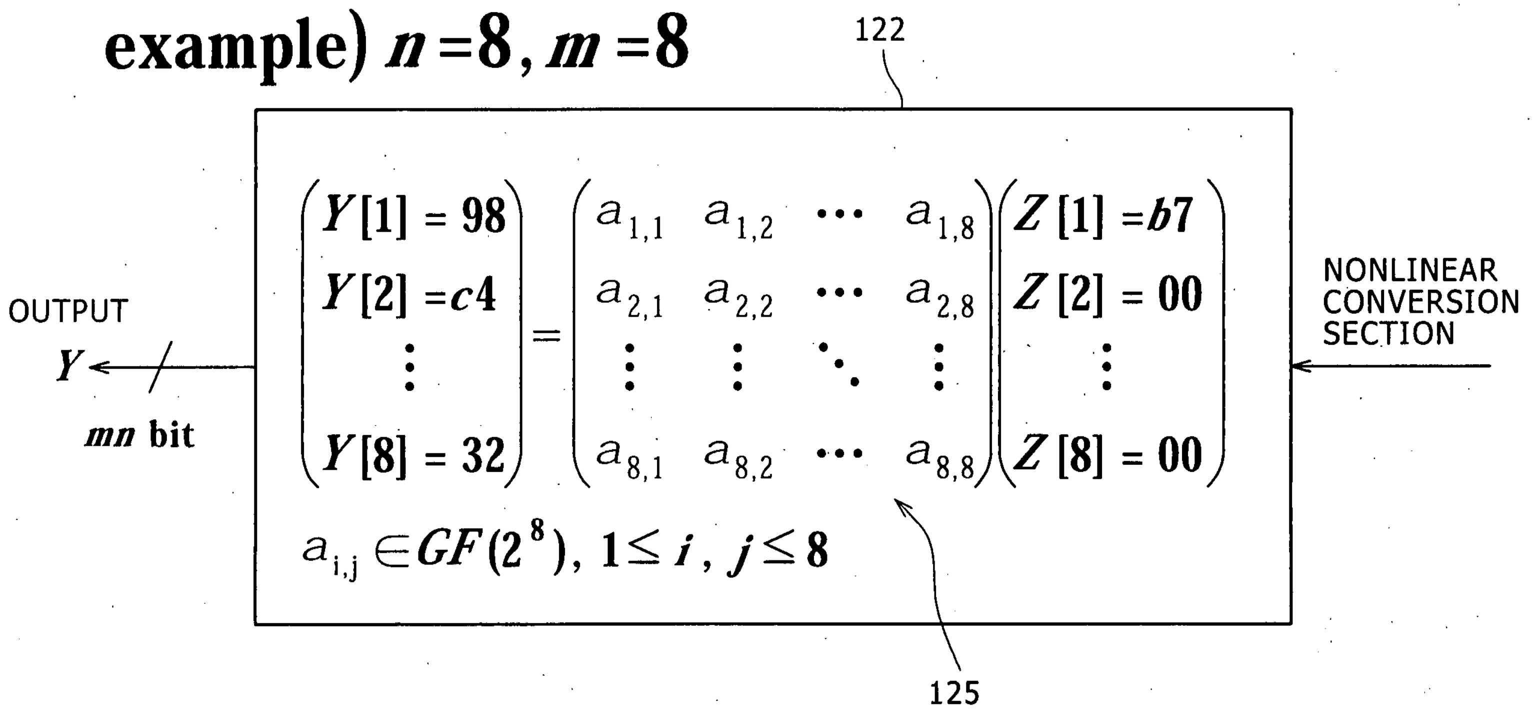

ΔX_{i-1} = (00,00,00,00,00,00,00,00)
ΔX_i = (34,00,00,00,00,00,00,00)
ΔY_i = (98,c4,b4,d3,ac,72,0f,32)
ΔX_i = (34,00,00,00,00,00,00,00)
131
ROUND i
K_i
34
S1
b7
00
S2~S8
00
LINEAR CONVERSION
ΔX_{i+1} = (98,c4,b4,d3,ac,72,0f,32)
ROUND i+1
K_{i+1}
S1 ~ S7
LINEAR CONVERSION
ΔY_{i+1} = (ad,00,00,00,00,00,00,00)
133
ROUND i+2
K_{i+2}
e1
S1
b7
00
S2~S8
00
LINEAR CONVERSION
ΔX_{i+2} = (e1,00,00,00,00,00,00,00)
ΔY_{i+2} = (98,c4,b4,d3,ac,72,0f,32)
OCCURRENCE OF SIMULTANEOUS DIFFERENCE VANISHMENT
ΔX_{i+3} = (00,00,00,00,00,00,00,00)
ΔX_{i+2} = (e1,00,00,00,00,00,00,00)

FIG.5



$$\begin{pmatrix} Y[1]=98 \\ Y[2]=c4 \\ \vdots \\ Y[8]=32 \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,8} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ a_{8,1} & a_{8,2} & \cdots & a_{8,8} \end{pmatrix} \begin{pmatrix} Z[1]=b7 \\ Z[2]=00 \\ \vdots \\ Z[8]=00 \end{pmatrix}$$

$$a_{i,j} \in GF(2^8),\ 1 \leq i,\ j \leq 8$$

FIG. 6

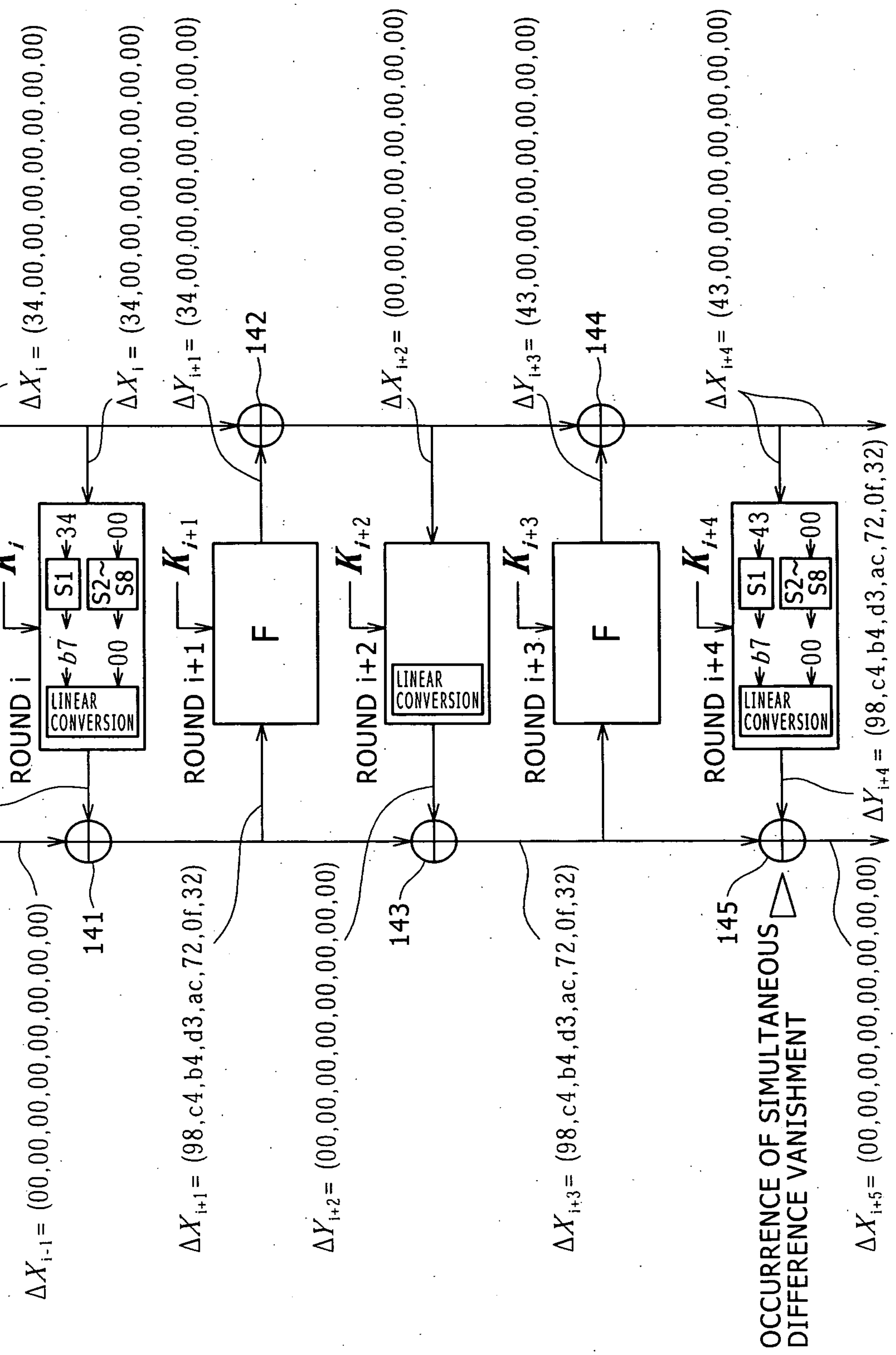

ΔX_{i-1} = (00,00,00,00,00,00,00,00)
ΔY_i = (98,c4,b4,d3,ac,72,0f,32)
ΔX_i = (34,00,00,00,00,00,00,00)
ΔX_i = (34,00,00,00,00,00,00,00)
141
ROUND i
K_i
34
00
S1
S2~S8
b7
00
LINEAR CONVERSION
ΔX_{i+1} = (98,c4,b4,d3,ac,72,0f,32)
ΔY_{i+1} = (34,00,00,00,00,00,00,00)
142
ROUND i+1
K_{i+1}
F
ΔY_{i+2} = (00,00,00,00,00,00,00,00)
ΔX_{i+2} = (00,00,00,00,00,00,00,00)
143
ROUND i+2
K_{i+2}
LINEAR CONVERSION
ΔX_{i+3} = (98,c4,b4,d3,ac,72,0f,32)
ΔY_{i+3} = (43,00,00,00,00,00,00,00)
144
ROUND i+3
K_{i+3}
F
ΔX_{i+4} = (43,00,00,00,00,00,00,00)
ROUND i+4
K_{i+4}
43
00
S1
S2~S8
b7
00
LINEAR CONVERSION
ΔY_{i+4} = (98,c4,b4,d3,ac,72,0f,32)
145
OCCURRENCE OF SIMULTANEOUS DIFFERENCE VANISHMENT
ΔX_{i+5} = (00,00,00,00,00,00,00,00)

FIG. 7

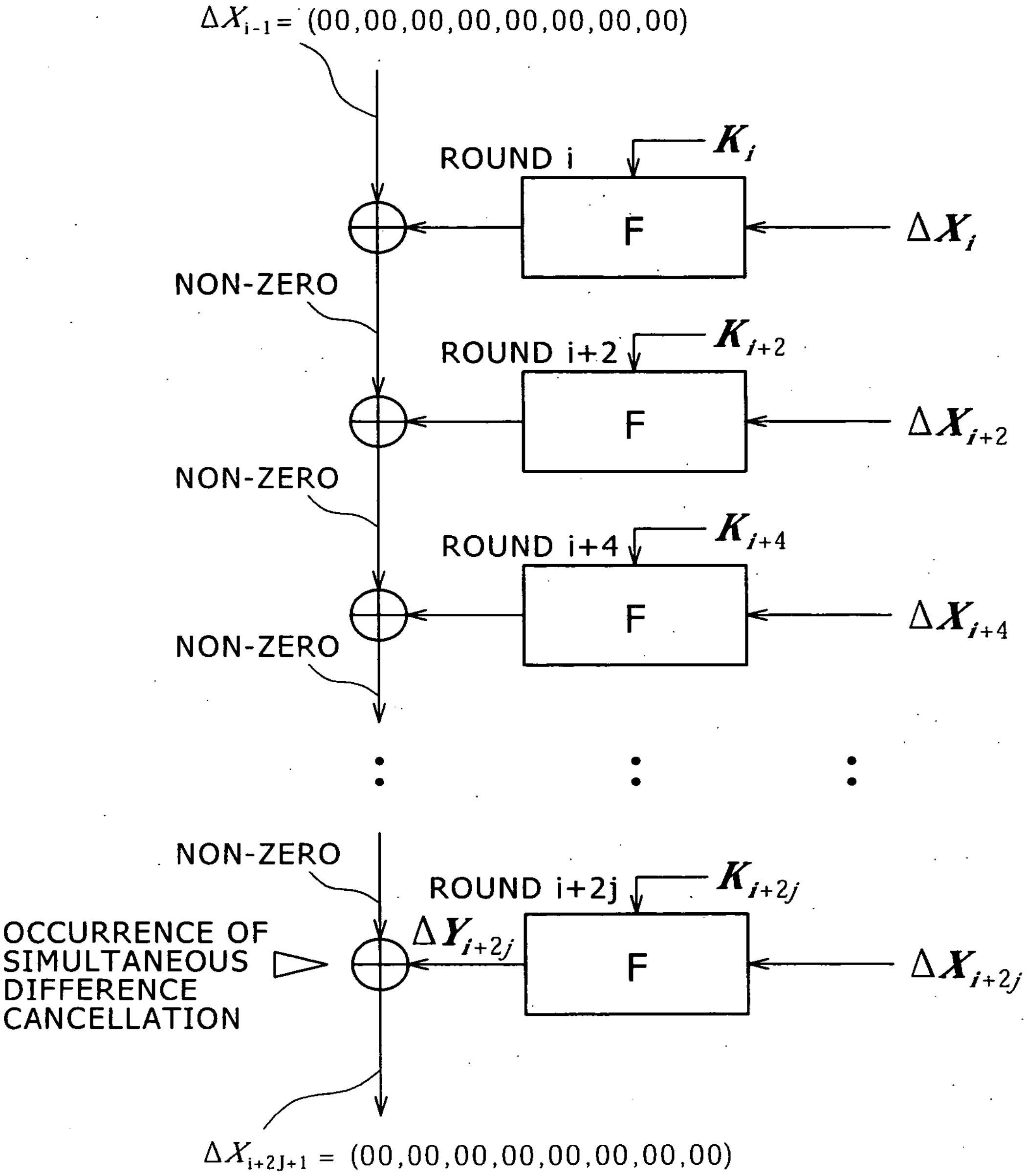

ΔX_{i-1} = (00,00,00,00,00,00,00,00)
ROUND i
K_i
F
ΔX_i
NON-ZERO
ROUND i+2
K_{i+2}
F
ΔX_{i+2}
NON-ZERO
ROUND i+4
K_{i+4}
F
ΔX_{i+4}
NON-ZERO
NON-ZERO
ROUND i+2j
K_{i+2j}
ΔY_{i+2j}
F
ΔX_{i+2j}
OCCURRENCE OF SIMULTANEOUS DIFFERENCE CANCELLATION
ΔX_{i+2J+1} = (00,00,00,00,00,00,00,00)

FIG.8

example) $n=8, m=8$

$$\begin{pmatrix}
9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\
29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\
67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\
8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\
d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\
2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\
42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\
55 & 63 & fa & 51 & c & d9 & 28 & d6
\end{pmatrix}$$

FIG. 9

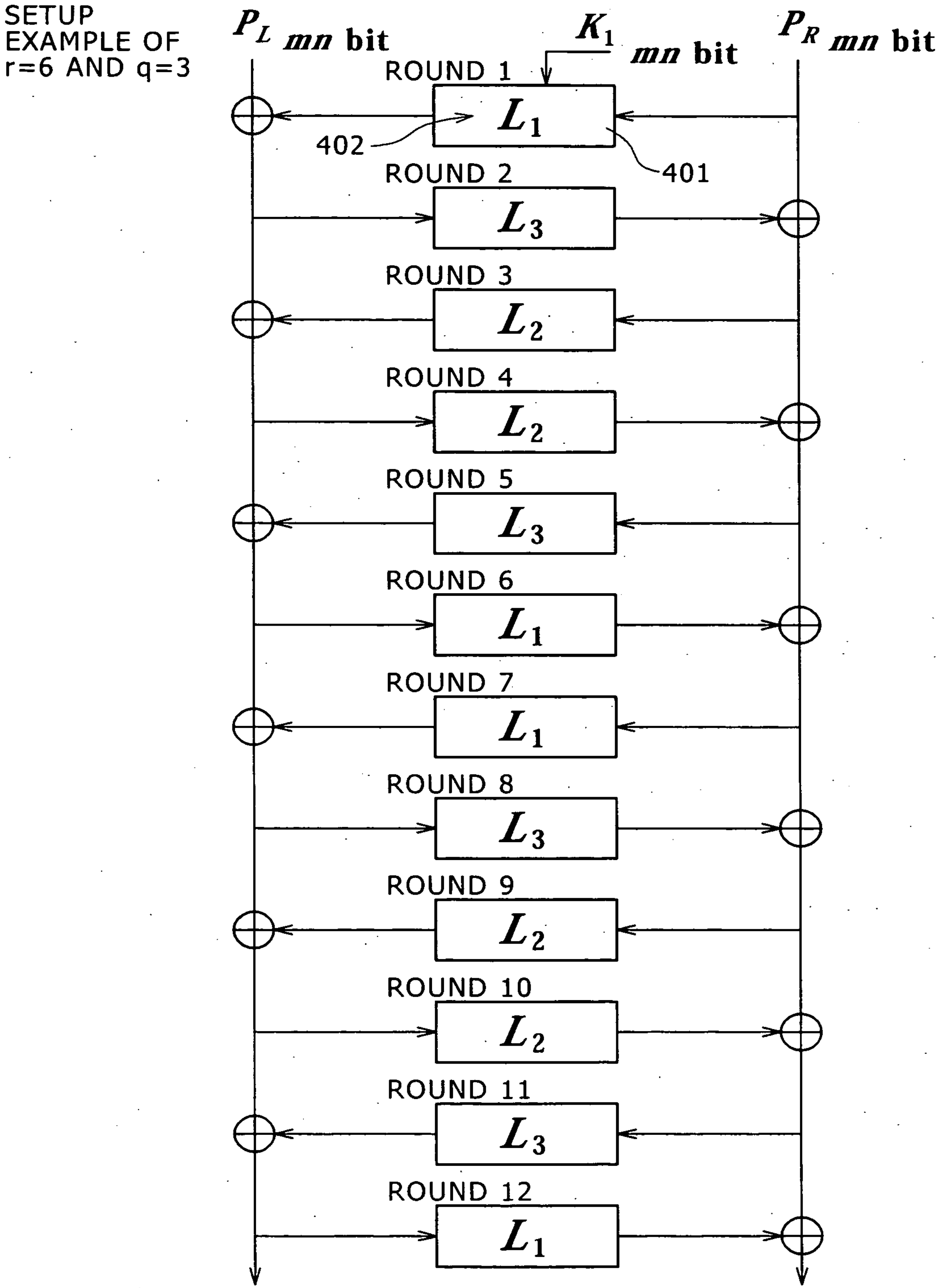

SETUP
EXAMPLE OF
r=6 AND q=3
P_L mn bit
K_1 mn bit
P_R mn bit
ROUND 1
L_1
402
401
ROUND 2
L_3
ROUND 3
L_2
ROUND 4
L_2
ROUND 5
L_3
ROUND 6
L_1
ROUND 7
L_1
ROUND 8
L_3
ROUND 9
L_2
ROUND 10
L_2
ROUND 11
L_3
ROUND 12
L_1

FIG. 10

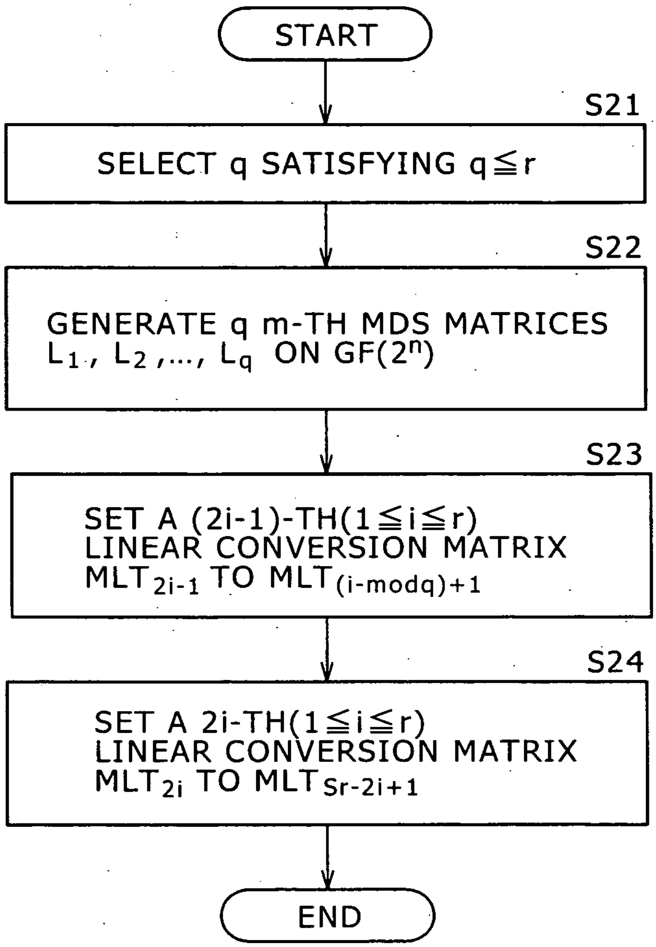
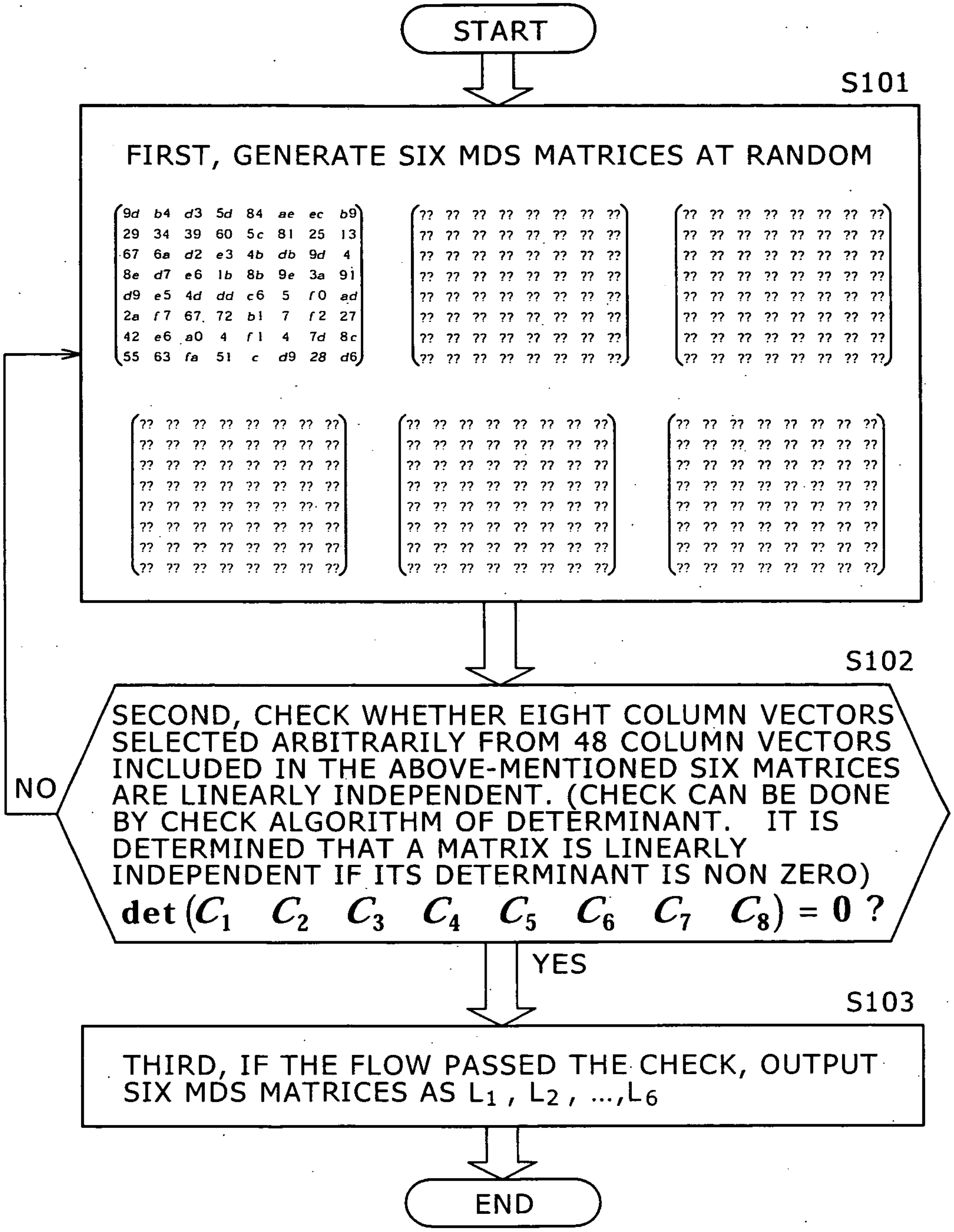

START
S21
SELECT q SATISFYING q≦r
S22
GENERATE q m-TH MDS MATRICES
L_1, L_2, ..., L_q ON GF(2^n)
S23
SET A (2i-1)-TH(1≦i≦r)
LINEAR CONVERSION MATRIX
MLT_{2i-1} TO $MLT_{(i\text{-}modq)+1}$
S24
SET A 2i-TH(1≦i≦r)
LINEAR CONVERSION MATRIX
MLT_{2i} TO $MLT_{Sr-2i+1}$
END

FIG. 11

CASE OF q=6, n=8, AND m=8



START

S101

FIRST, GENERATE SIX MDS MATRICES AT RANDOM

$$\begin{pmatrix} 9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\ 29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\ 67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\ 8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\ d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\ 2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\ 42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\ 55 & 63 & fa & 51 & c & d9 & 28 & d6 \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

$$\begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

S102

SECOND, CHECK WHETHER EIGHT COLUMN VECTORS SELECTED ARBITRARILY FROM 48 COLUMN VECTORS INCLUDED IN THE ABOVE-MENTIONED SIX MATRICES ARE LINEARLY INDEPENDENT. (CHECK CAN BE DONE BY CHECK ALGORITHM OF DETERMINANT. IT IS DETERMINED THAT A MATRIX IS LINEARLY INDEPENDENT IF ITS DETERMINANT IS NON ZERO)

$$\det\left(C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \quad C_6 \quad C_7 \quad C_8\right) = 0\ ?$$

NO

YES

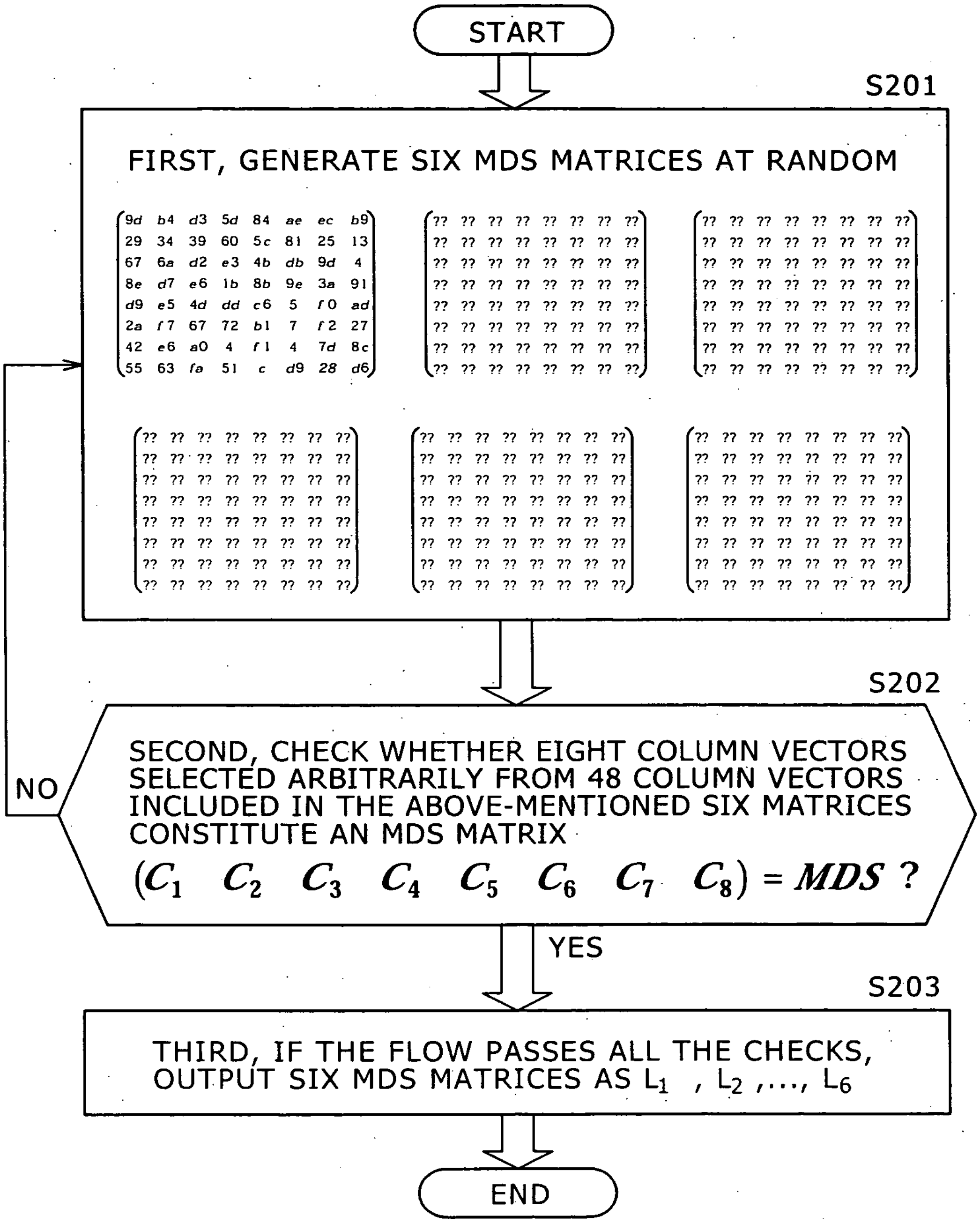
S103

THIRD, IF THE FLOW PASSED THE CHECK, OUTPUT SIX MDS MATRICES AS L_1, L_2, …, L_6

END

FIG. 12

CASE OF q=6, n=8, AND m=8



FIRST, GENERATE SIX MDS MATRICES AT RANDOM

$$\begin{pmatrix} 9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\ 29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\ 67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\ 8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\ d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\ 2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\ 42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\ 55 & 63 & fa & 51 & c & d9 & 28 & d6 \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

$$\begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \quad \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

SECOND, CHECK WHETHER EIGHT COLUMN VECTORS SELECTED ARBITRARILY FROM 48 COLUMN VECTORS INCLUDED IN THE ABOVE-MENTIONED SIX MATRICES CONSTITUTE AN MDS MATRIX

$$(C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \quad C_6 \quad C_7 \quad C_8) = MDS\ ?$$

THIRD, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS L_1 , L_2 ,..., L_6

FIG. 13

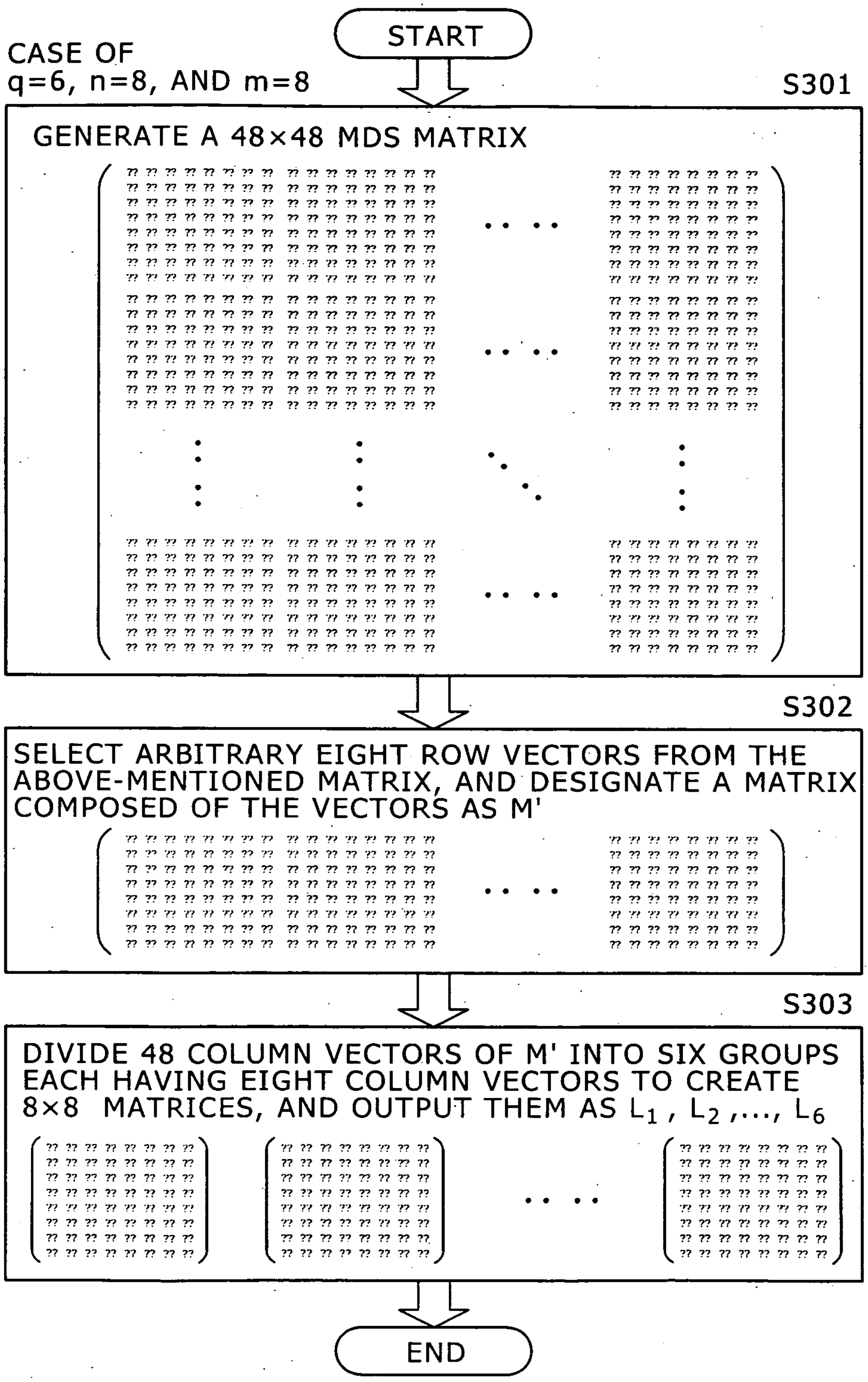

START
CASE OF
q=6, n=8, AND m=8
S301
GENERATE A 48×48 MDS MATRIX
S302
SELECT ARBITRARY EIGHT ROW VECTORS FROM THE ABOVE-MENTIONED MATRIX, AND DESIGNATE A MATRIX COMPOSED OF THE VECTORS AS M'
S303
DIVIDE 48 COLUMN VECTORS OF M' INTO SIX GROUPS EACH HAVING EIGHT COLUMN VECTORS TO CREATE 8×8 MATRICES, AND OUTPUT THEM AS L1, L2, ..., L6
END

FIG. 14

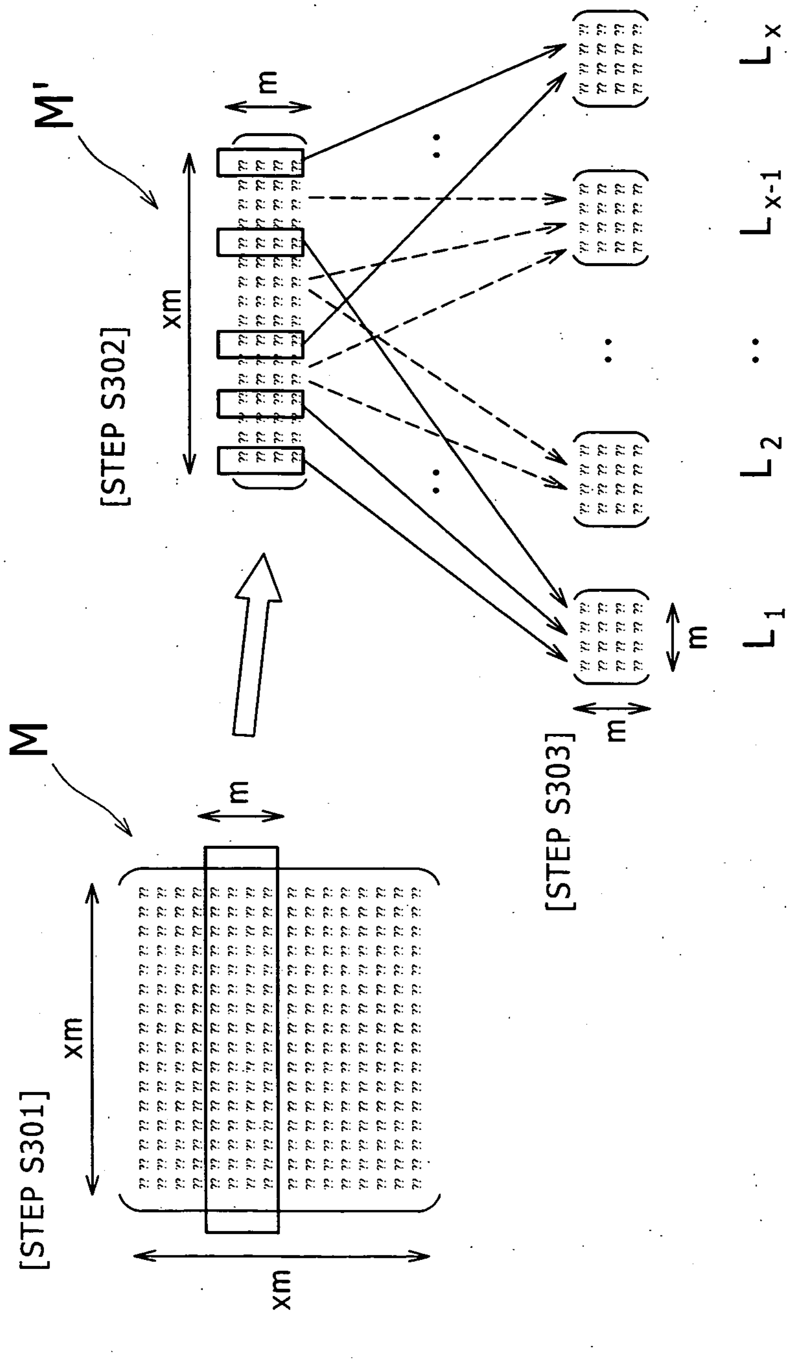
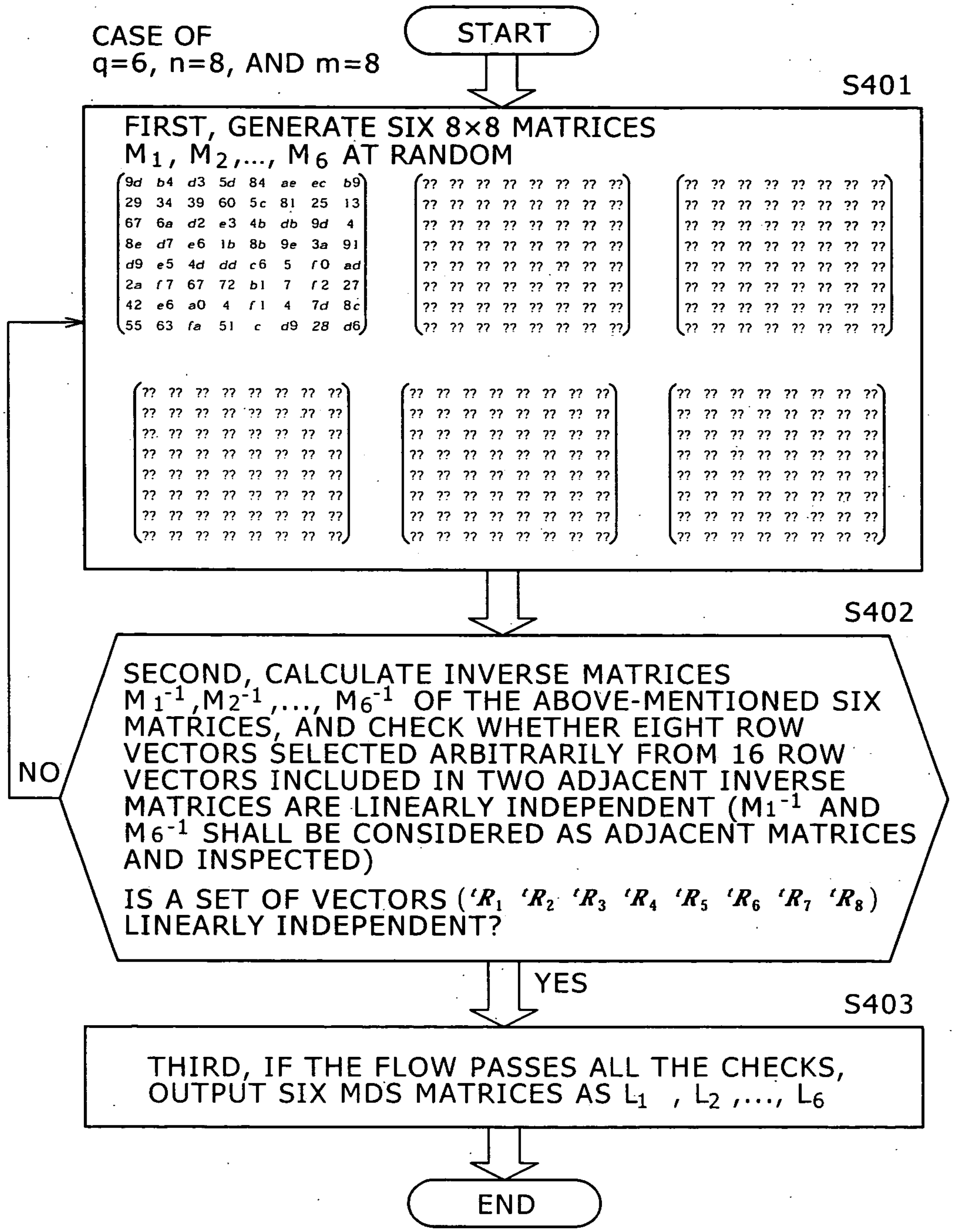


FIG. 15



CASE OF $q=6$, $n=8$, AND $m=8$

FIRST, GENERATE SIX 8×8 MATRICES $M_1, M_2, \ldots, M_6$ AT RANDOM

$$\begin{pmatrix} 9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\ 29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\ 67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\ 8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\ d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\ 2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\ 42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\ 55 & 63 & fa & 51 & c & d9 & 28 & d6 \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

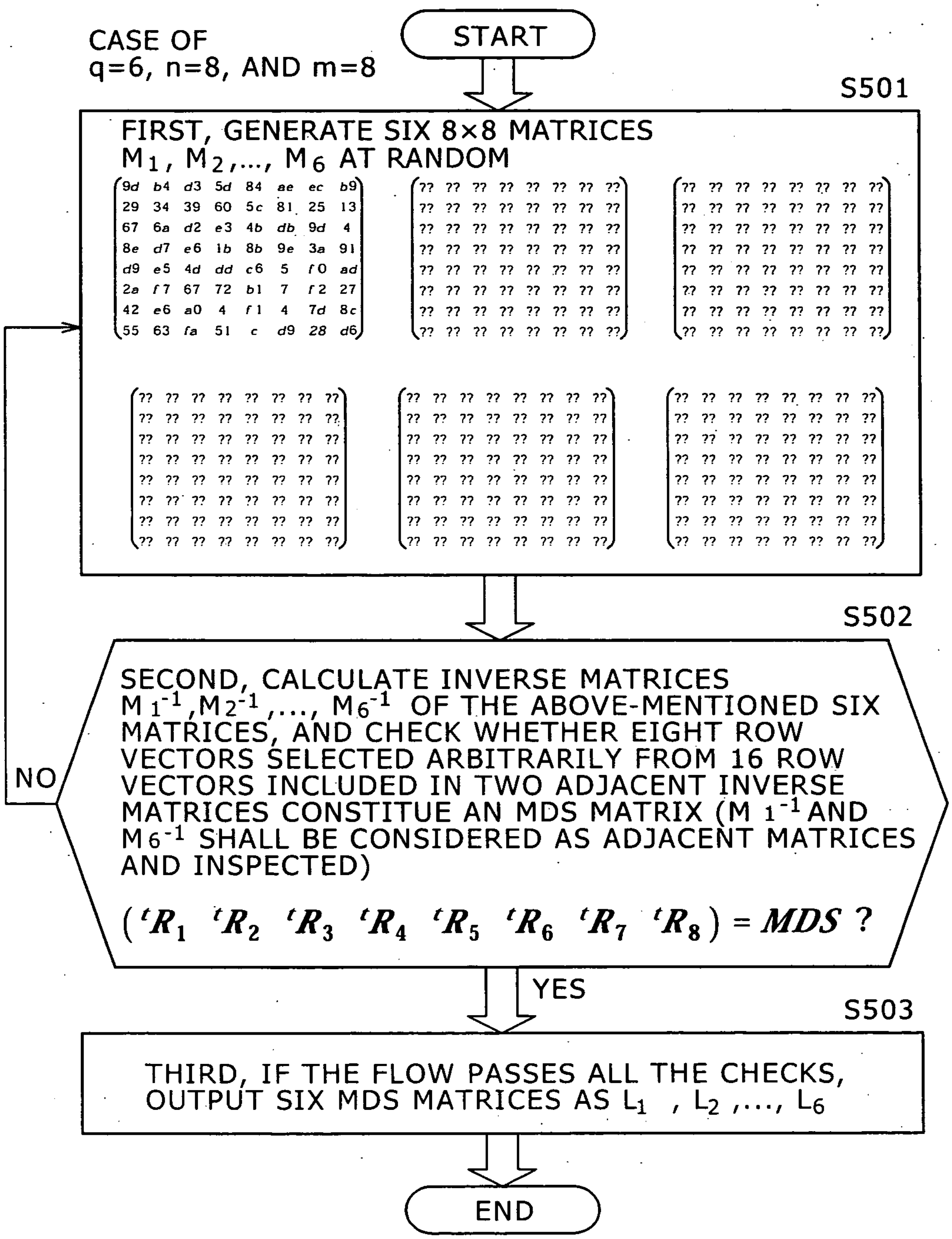
$$\begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

SECOND, CALCULATE INVERSE MATRICES $M_1^{-1}, M_2^{-1}, \ldots, M_6^{-1}$ OF THE ABOVE-MENTIONED SIX MATRICES, AND CHECK WHETHER EIGHT ROW VECTORS SELECTED ARBITRARILY FROM 16 ROW VECTORS INCLUDED IN TWO ADJACENT INVERSE MATRICES ARE LINEARLY INDEPENDENT (M_1^{-1} AND M_6^{-1} SHALL BE CONSIDERED AS ADJACENT MATRICES AND INSPECTED)

IS A SET OF VECTORS (${}^t\boldsymbol{R}_1$ ${}^t\boldsymbol{R}_2$ ${}^t\boldsymbol{R}_3$ ${}^t\boldsymbol{R}_4$ ${}^t\boldsymbol{R}_5$ ${}^t\boldsymbol{R}_6$ ${}^t\boldsymbol{R}_7$ ${}^t\boldsymbol{R}_8$) LINEARLY INDEPENDENT?

THIRD, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS L_1, L_2, …, L_6

FIG.16


CASE OF
q=6, n=8, AND m=8
START
S501
FIRST, GENERATE SIX 8×8 MATRICES
$M_1, M_2, \ldots, M_6$ AT RANDOM
S502
SECOND, CALCULATE INVERSE MATRICES $M_1^{-1}, M_2^{-1}, \ldots, M_6^{-1}$ OF THE ABOVE-MENTIONED SIX MATRICES, AND CHECK WHETHER EIGHT ROW VECTORS SELECTED ARBITRARILY FROM 16 ROW VECTORS INCLUDED IN TWO ADJACENT INVERSE MATRICES CONSTITUE AN MDS MATRIX (M_1^{-1} AND M_6^{-1} SHALL BE CONSIDERED AS ADJACENT MATRICES AND INSPECTED)
$({}^tR_1 \ {}^tR_2 \ {}^tR_3 \ {}^tR_4 \ {}^tR_5 \ {}^tR_6 \ {}^tR_7 \ {}^tR_8) = MDS$?
NO
YES
S503
THIRD, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS $L_1, L_2, \ldots, L_6$
END

$$\begin{pmatrix} 9d & b4 & d3 & 5d & 84 & ae & ec & b9 \\ 29 & 34 & 39 & 60 & 5c & 81 & 25 & 13 \\ 67 & 6a & d2 & e3 & 4b & db & 9d & 4 \\ 8e & d7 & e6 & 1b & 8b & 9e & 3a & 91 \\ d9 & e5 & 4d & dd & c6 & 5 & f0 & ad \\ 2a & f7 & 67 & 72 & b1 & 7 & f2 & 27 \\ 42 & e6 & a0 & 4 & f1 & 4 & 7d & 8c \\ 55 & 63 & fa & 51 & c & d9 & 28 & d6 \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

$$\begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix} \begin{pmatrix} ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \\ ?? & ?? & ?? & ?? & ?? & ?? & ?? & ?? \end{pmatrix}$$

FIG. 17

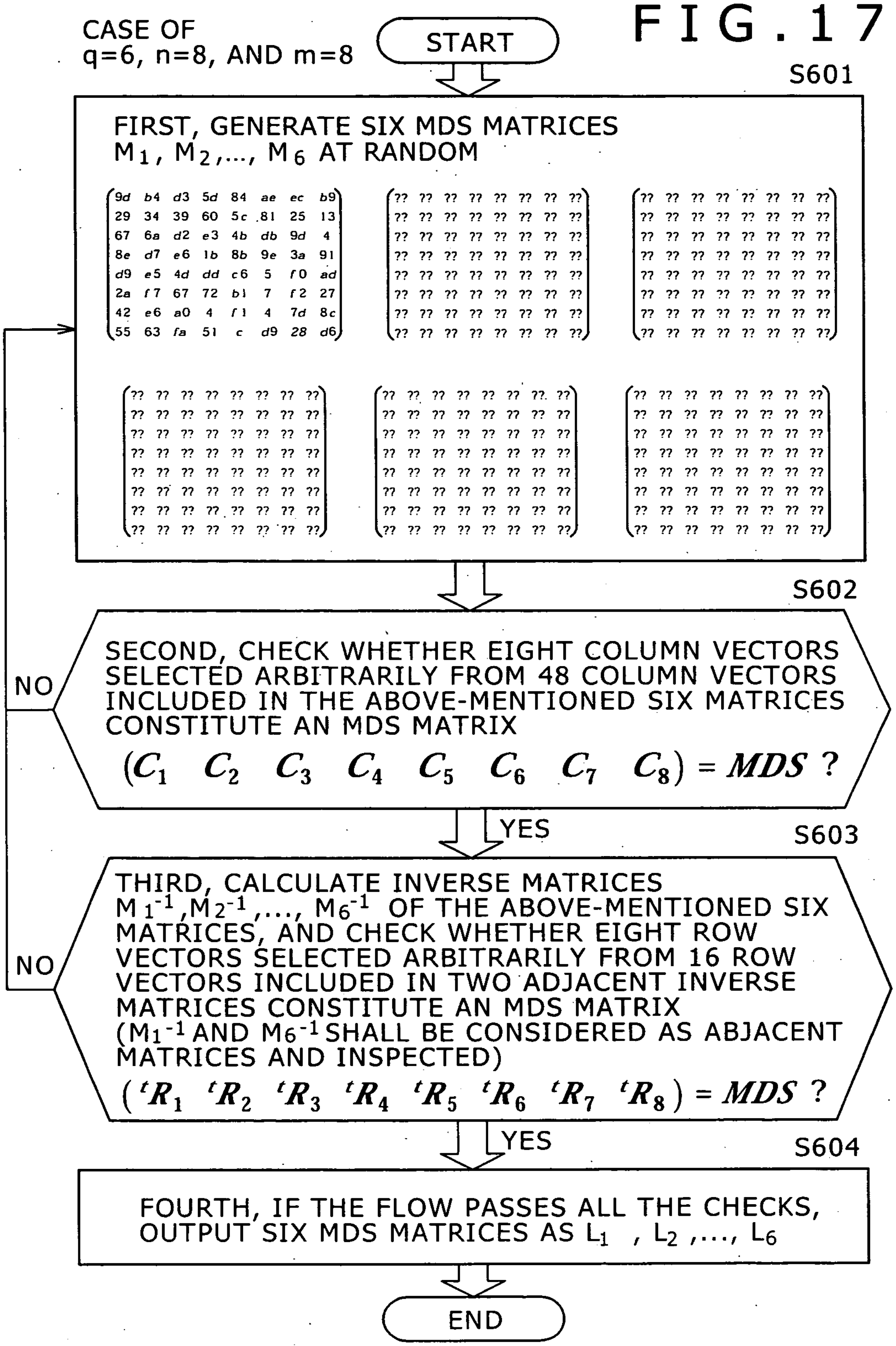
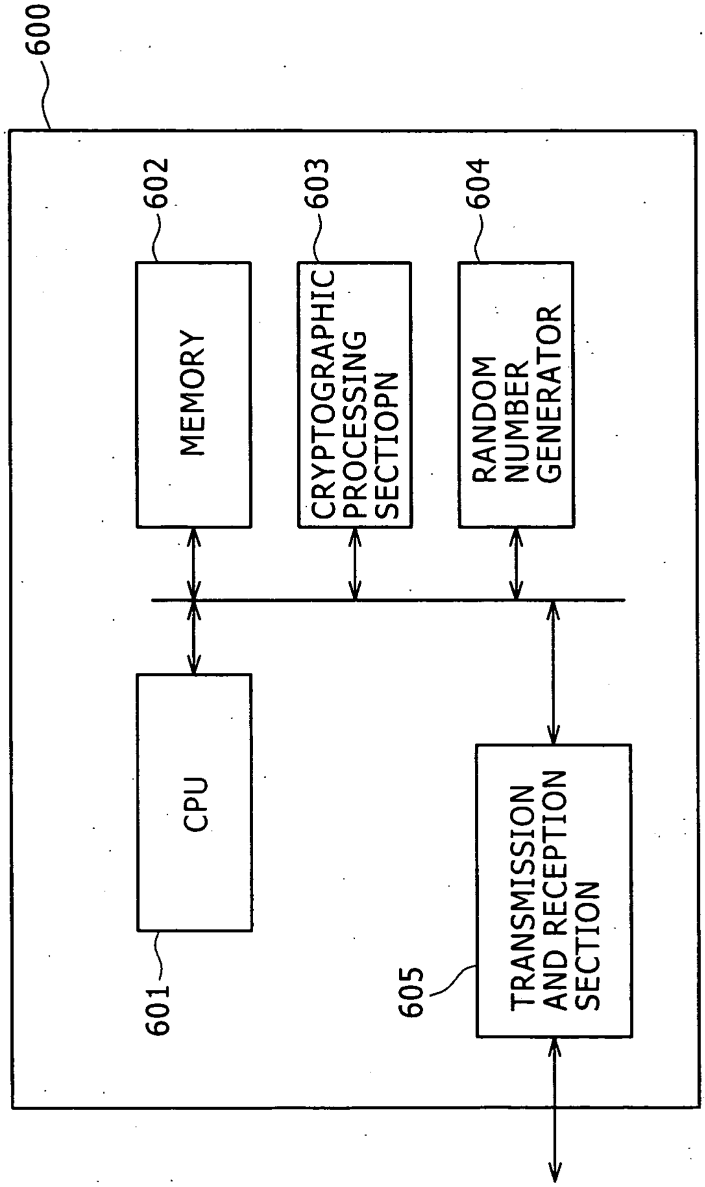

CASE OF
q=6, n=8, AND m=8
START
S601
FIRST, GENERATE SIX MDS MATRICES
M1, M2,..., M6 AT RANDOM
9d b4 d3 5d 84 ae ec b9
29 34 39 60 5c 81 25 13
67 6a d2 e3 4b db 9d 4
8e d7 e6 1b 8b 9e 3a 91
d9 e5 4d dd c6 5 f0 ad
2a f7 67 72 b1 7 f2 27
42 e6 a0 4 f1 4 7d 8c
55 63 fa 51 c d9 28 d6
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ??
S602
SECOND, CHECK WHETHER EIGHT COLUMN VECTORS SELECTED ARBITRARILY FROM 48 COLUMN VECTORS INCLUDED IN THE ABOVE-MENTIONED SIX MATRICES CONSTITUTE AN MDS MATRIX
(C1 C2 C3 C4 C5 C6 C7 C8) = MDS ?
NO
YES
S603
THIRD, CALCULATE INVERSE MATRICES M1-1, M2-1,..., M6-1 OF THE ABOVE-MENTIONED SIX MATRICES, AND CHECK WHETHER EIGHT ROW VECTORS SELECTED ARBITRARILY FROM 16 ROW VECTORS INCLUDED IN TWO ADJACENT INVERSE MATRICES CONSTITUTE AN MDS MATRIX
(M1-1 AND M6-1 SHALL BE CONSIDERED AS ABJACENT MATRICES AND INSPECTED)
(tR1 tR2 tR3 tR4 tR5 tR6 tR7 tR8) = MDS ?
NO
YES
S604
FOURTH, IF THE FLOW PASSES ALL THE CHECKS, OUTPUT SIX MDS MATRICES AS L1, L2,..., L6
END

FIG.18


600
602
MEMORY
603
CRYPTOGRAPHIC PROCESSING SECTIOPN
604
RANDOM NUMBER GENERATOR
CPU
601
605
TRANSMISSION AND RECEPTION SECTION